

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

This Page Blank (uspto)

ABSTRACTED-PUB-NO: JP09046672A

BASIC-ABSTRACT:

The apparatus has a scramble key with extractor having and encrypted encipherment device which changes and boosts a scrambler (3). A

de-scrambler is included in a decoder (31) which decodes the encrypted scramble key changed by the encipherment device.

ADVANTAGE - Enables careless decoding of scramble key. Prevents excessive use of scramble key.

CHOSEN-DRAWING: Dwg. 1/5

TITLE-TERMS: APPARATUS BROADCAST STATION DECODE DECODE
ENCRYPTION SCRAMBLE KEY CHANGE BOOST DEVICE

This Page Blank (uspto)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 9 - 4 6 6 7 2

(43) 公開日 平成 9 年 (1 9 9 7) 2 月 1 4 日

(51) Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H04N 7/16			H04N 7/16	A
H04H 1/00			H04H 1/00	F

審査請求 未請求 請求項の数 2 O L (全 7 頁)

(21) 出願番号 特願平 7 - 1 9 1 4 4 9

(22) 出願日 平成 7 年 (1 9 9 5) 7 月 2 7 日

(71) 出願人 0 0 0 0 0 2 1 8 5
ソニー株式会社
東京都品川区北品川 6 丁目 7 番 3 5 号

(72) 発明者 吉田 洋之
東京都品川区北品川 6 丁目 7 番 3 5 号 ソ
ニー株式会社内

(72) 発明者 城間 真
東京都品川区北品川 6 丁目 7 番 3 5 号 ソ
ニー株式会社内

(72) 発明者 山下 雅美
東京都品川区北品川 6 丁目 7 番 3 5 号 ソ
ニー株式会社内

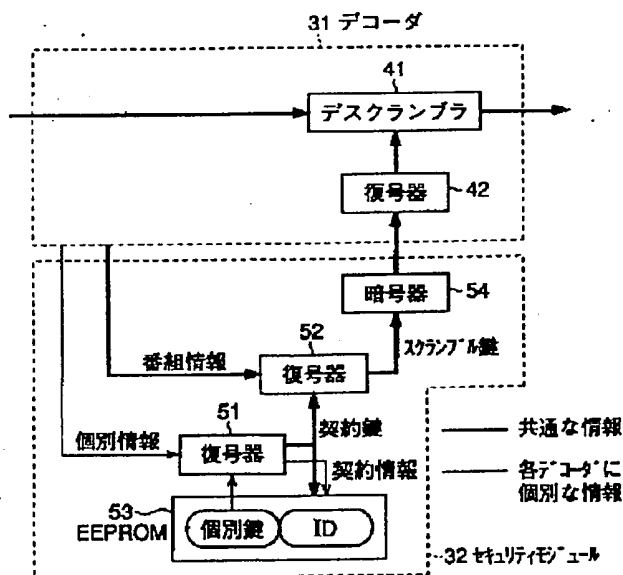
(74) 代理人 弁理士 稲本 義雄

(54) 【発明の名称】 デスクランブル装置および方法

(57) 【要約】

【課題】 スクランブル鍵が盗用されるのを抑制する。

【解決手段】 デコーダ 31 に対して装着される IC カードなどよりなるセキュリティモジュール 32 に、暗号器 54 を設ける。この暗号器 54 により、スクランブル鍵を暗号化してデコーダ 31 に出力する。デコーダ 31 においては、復号器 42 で、この暗号化されたスクランブル鍵を復号化し、デスクランブラ 41 に供給する。デスクランブラ 41 は、復号器 42 より供給されたスクランブル鍵を用いて、スクランブルされているデータをデスクランブルする。



【特許請求の範囲】

【請求項 1】 放送されてきた複数の情報を分離するとともに、スクランブルされている所定のチャンネルの番組の情報をデスクランブルするデスクランブル手段と、前記デスクランブル手段に対して着脱され、放送されてきた情報から前記スクランブルを解除するためのスクランブル鍵を抽出し、前記デスクランブル手段に供給する抽出手段とを備えるデスクランブル装置において、前記抽出手段は、前記スクランブル鍵を暗号化して前記スクランブル手段に供給する暗号化手段を備え、前記デスクランブル手段は、前記暗号化手段により暗号化された前記スクランブル鍵を、復号化する復号化手段を備えることを特徴とするデスクランブル装置。

【請求項 2】 放送されてきた複数の情報を分離するとともに、スクランブルされている所定のチャンネルの番組の情報をデスクランブルするデスクランブル手段と、前記デスクランブル手段に対して着脱され、放送されてきた情報から前記スクランブルを解除するためのスクランブル鍵を抽出し、前記デスクランブル手段に供給する抽出手段とを備えるデスクランブル装置のデスクランブル方法において、前記抽出手段において、前記スクランブル鍵を暗号化して前記スクランブル手段に供給し、前記デスクランブル手段において、暗号化された前記スクランブル鍵を、復号化することを特徴とするデスクランブル方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デスクランブル装置および方法に関し、特にスクランブル鍵が不用意に解読され、不正に利用されるのを抑制するようにしたデスクランブル装置および方法に関する。

【0002】

【従来の技術】有料放送においては、スクランブル放送と呼ばれる放送方式が用いられることが多い。このスクランブル放送は、放送局側において、元の信号を所定の方法で意図的に乱す（スクランブルする）ことにより、放送局と契約していない者が放送を受信しても、正常な画像、音声、およびデータなどを利用することができないようにするものである。

【0003】すなわち、放送局と契約した者のデコーダに対しては、このスクランブルを解除する鍵信号を与え、この鍵信号によりデコーダがスクランブルされているデータを元の形にデスクランブルすることで、正常な画像、音声、およびデータなどを得ることができるようにしている。

【0004】有料放送を視聴する契約のうち、チャンネル単位で契約する場合をフラット、視聴した番組に応じて課金される場合をペイパービューという。ペイパービューのうち、視聴者が急に所定の番組を見なくなった場

合、所定の操作を行うだけでそれを見ることができる、事前連絡が不要のものを特にインパルスペイパービューといい、事前連絡が必要なものを、コールアヘッドペイパービューという。

【0005】

【発明が解決しようとする課題】このように、スクランブル放送をデスクランブルするには、鍵信号が必要となるが、従来のスクランブル装置においては、この鍵が不正に取得され、視聴契約をしていない者が、スクランブル放送を不正に視聴するおそれがあった。

【0006】本発明はこのような状況に鑑みてなされたものであり、視聴契約をしていない番組が、不正に視聴されることを抑制するものである。

【0007】

【課題を解決するための手段】請求項 1 に記載のデスクランブル装置は、抽出手段は、スクランブル鍵を暗号化してスクランブル手段に供給する暗号化手段を備え、デスクランブル手段は、暗号化手段により暗号化されたスクランブル鍵を、復号化する復号化手段を備えることを特徴とする。

【0008】請求項 2 に記載のデスクランブル方法は、抽出手段において、スクランブル鍵を暗号化してスクランブル手段に供給し、デスクランブル手段において、暗号化されたスクランブル鍵を、復号化することを特徴とする。

【0009】請求項 1 に記載のデスクランブル装置においては、抽出手段が、スクランブル鍵を暗号化してスクランブル手段に供給する暗号化手段を備え、デスクランブル手段が、暗号化手段により暗号化されたスクランブル鍵を、復号化する復号化手段を備える。

【0010】請求項 2 に記載のデスクランブル方法においては、抽出手段において、スクランブル鍵を暗号化してスクランブル手段に供給し、デスクランブル手段において、暗号化されたスクランブル鍵を、復号化する。

【0011】

【発明の実施の形態】図 1 は、本発明を応用した有料放送システムの一実施例の構成を示すブロック図である。送信側システム 21 のエンコーダ 1（1A 乃至 1E）は、5 チャンネル分の映像信号や音声信号をデジタル化し、圧縮するようになされている。多重化器 2 は、複数（5 チャンネル分）のエンコーダ 1 の出力や複数の関連情報をパケット化し、時分割多重する。ここで関連情報とは、番組に関する情報とデスクランブルのためのスクランブル鍵を含む「共通情報（番組情報）」、加入者（視聴者）毎の契約情報（例えばフラットやペイパービューなどの契約形態など）および共通情報の暗号を解くための契約鍵を含む「個別情報」などからなるものとする。

【0012】スクランブラ 3 は、関連情報送出装置 4 からのスクランブル鍵により、多重化器 2 の出力信号の所

定のものに対して選択的にスクランブルを施すようになされている。

【0013】スクランブル制御システム6は、関連情報送出装置4に契約鍵（ワーク鍵）を供給するとともに、受信端末22に固有の個別鍵（スクランブル制御システム6に記憶されている）により契約鍵を暗号化し、個別情報の一部として多重化器2に供給するようになされている。

【0014】関連情報送出装置4は、スクランブラ3にスクランブル鍵を供給するとともに、スクランブル制御システム6から供給された契約鍵により、スクランブル鍵を暗号化し、共通情報（番組情報）の一部として多重化器2に供給するようになされている。

【0015】番組制御システム5は、所定の制御信号を発生し、番組に応じてエンコーダ1を制御する。すなわち、デジタル化や圧縮の方法を制御する。また、いま、エンコーダ1においてエンコードされている番組の番組IDや対応するチャンネルのチャンネルID（service-id）等を発生し、関連情報送出装置4に供給する。視聴情報収集処理システム7は、多数の受信端末22から電話回線24を介してアップロードされる視聴情報（例えば視聴した番組ID、対応するチャンネルID、および視聴した時間など）や、視聴者からの契約要求を処理し、契約情報としてスクランブル制御システム6に供給するようになされている。

【0016】一方、受信端末22のデコーダ31（デスクランブル手段）は、内蔵するデスクランブラ41（図4）により、セキュリティモジュール32（抽出手段）から供給されたスクランブル鍵により、スクランブルされた信号を元の信号にデスクランブルするようになされている。また、番組に付加された個別情報や番組情報を抽出し、出力するようになされている。

【0017】セキュリティモジュール32は、デコーダ31に対して着脱自在に装着される例えばICカード等により構成され、内蔵するEEPROM53（図4）に、受信端末22に固有の個別鍵を記憶しており、デコーダ31よりスクランブルされていない個別情報が供給されたとき、この個別鍵を用いて個別情報を復号し、契約鍵と契約情報をそれぞれ取り出し、記憶する。また、デコーダ31を介して供給された番組に付随する共通情報を取り込み、契約鍵により共通情報を復号し、スクランブル鍵を取り出し、暗号化した後、デコーダ31に供給するようになされている。

【0018】次にその動作について説明する。まず、送信側システム21より受信端末22に個別情報が送信される場合の動作について説明する。この個別情報は、図2に示すように、契約鍵に対応する契約鍵番号、契約鍵、契約したチャンネルに対応するチャンネルID（service-id）、および契約タイプなどを含んでいる。また、個別情報は、送信先の受信端末22のID

番号（Card ID）も含んでいる。

【0019】契約鍵は、例えば、8ビットの契約鍵番号とともに送信され、複数の契約鍵を使い分けることができるようになっている。契約したチャンネルIDを、例えば16ビットのService_idで表すものとする。契約タイプは、フラット、ペイパービュー、特別契約を識別することができるもので、例えば4ビットとする。

【0020】この個別情報は、スクランブル制御システム6において、この個別情報が送信されるべき送信先の受信端末22に固有の個別鍵を用いて暗号化される。スクランブル制御システム6は、全ての受信端末22について、受信端末22に固有の個別鍵を受信端末22のID番号（Card ID）に対応させて記憶しており、送信先の受信端末22のID番号からその個別鍵を検索することができるようになっている。従って、送信先の受信端末22のID番号に対応する個別鍵を検索し、それに基づいて、個別情報が暗号化されることになる。暗号化された個別情報は多重化器2に供給される。

【0021】多重化器2においては、エンコーダ1より供給された所定の番組に対応するデジタル化され、圧縮された映像信号や音声信号と、スクランブル制御システム6より供給された個別情報がパケット化され、時分割多重された後、スクランブラ3に供給される。スクランブラ3に供給されたデジタル信号は、関連情報送出装置4より供給されたスクランブル鍵を用いて番組部分（映像データと音声データ）だけがスクランブルされ、個別情報の部分はスクランブルされずに伝送路23に送出される。

【0022】なお、この個別情報の受信端末22への送信は、個別情報の更新が必要とされる時に、必要に応じて随時行われる。この個別情報には、上述した契約情報が含まれている。

【0023】次に、通常の番組とそれに付加された番組情報（共通情報の構成要素）が送信側システム21から受信端末22に送信される場合の動作について説明する。

【0024】番組情報は、例えば図3に示すように、契約タイプ、契約鍵の番号を示す契約鍵番号、スクランブル鍵、チャンネルIDに相当するService_id、番組を識別するための番組IDなどを含んでいる。このうちスクランブル鍵は、スクランブル制御システム6より供給された契約鍵（ワーク鍵）によって暗号化されている。また、契約タイプには、特別番組であるか否かを識別するためのフラグが含まれている。

【0025】関連情報送出装置4において生成された上述したような構成の所定の番組情報は、多重化器2に供給される。多重化器2においては、エンコーダ1から供給された所定の番組に対応するデジタル化され、圧縮された映像信号や音声信号と、関連情報送出装置4より

供給された番組情報がバケット化され、時分割多重され、スクランブラ 3 に供給される。

【0026】スクランブラ 3 には、番組を構成する圧縮された映像信号や音声信号と番組情報がバケット化され、時分割多重されたデジタル信号が入力されるが、このうちの番組部分（映像信号と音声信号）だけが関連情報送出装置 4 より供給されたスクランブル鍵によってスクランブルされ、番組情報の部分はスクランブルされずに伝送路 2 3 に送出される。

【0027】このようにして、所定の番組とそれに付随する番組情報が送信側システム 2 1 より受信端末 2 2 に送信される。

【0028】次に、受信端末 2 2 側の動作について説明する。

【0029】図 4 は、受信端末 2 2 において、視聴許可の制御を行う場合の原理的な動作を説明するための図である。デコーダ 3 1 は、例えば、デスクランブラ 4 1 と復号器 4 2（復号化手段）により構成され、セキュリティモジュール 3 2 は、復号器 5 1、5 2、EEPROM 5 3 および暗号器 5 4（暗号化手段）より構成されてい

る。

【0030】正式に契約した視聴者の受信端末 2 2 には、個別情報が送信される。送信側システム 2 1 より、伝送路 2 3 を介して送信されたスクランブルされた所定の番組と、スクランブルされていない個別情報が時分割多重されたデジタル信号が、受信端末 2 2 の図示せぬチューナにより受信されると、スクランブルされた番組に対応するデジタル信号は、デスクランブラ 4 1 に供給される。

【0031】一方、スクランブルされていない個別情報の非暗号部に付加された受信端末 2 2 の ID 番号（Card ID）と、セキュリティモジュール 3 2 の EEPROM 5 3 に予め記憶されている受信端末 2 2 の ID 番号（Card ID）とが比較され、両者が一致した場合、その個別情報が（すなわち自分自身宛の個別情報が）取り込まれ、復号器 5 1 に供給される。

【0032】復号器 5 1 に供給された個別情報のうち、暗号化されている部分は、EEPROM 5 3 に記憶されている受信端末 2 2 に固有の個別鍵によって解読され、契約鍵、および契約情報が取り出され、EEPROM 5 3 に供給され、記憶される。この契約鍵は、番組情報の解読に使用される。また、契約情報は、受信した番組が契約した番組であるか否かを判断するとき使用される。

【0033】受信端末 2 2 において、視聴者が番組を視聴しているとき、受信端末 2 2 は、伝送路 2 3 を介して送信されてきたスクランブルされた所定の番組と、それに付随した番組情報を受信している。スクランブルされた所定の番組に対応するデジタル信号は、デスクランブラ 4 1 に供給され、それに付随した番組情報は、復号器 5 2 に供給される。

【0034】所定の番組のチャンネルに対応する契約鍵が、上述したようにして、すでに復号器 5 1 において復号され、EEPROM 5 3 に記憶されている場合、復号器 5 2 が動作し、EEPROM 5 3 より供給されたその契約鍵によって番組情報のうちの暗号化されている部分が復号化される。これにより、番組情報に含まれているスクランブル鍵が取り出される。

【0035】復号器 5 2 により復号化されたスクランブル鍵は、暗号器 5 4 に入力され、暗号化される。この暗号化には、EEPROM 5 3 に記憶されている Card ID と Ca__System__ID（これについては、後述する）の少なくとも一方が利用される。

【0036】この場合、Card ID と Ca__System__ID の少なくとも一方を、そのまま暗号化のための鍵として用いたり、所定の演算を施すことにより、暗号化を行うことができる。

【0037】次に、番組情報は、EEPROM 5 3 にすでに記憶している契約情報との照合が行われる。照合の結果、番組情報が付加された番組が、契約した番組であると認識された場合、暗号器 5 4 において得られたスクランブル鍵（暗号化されている）は、セキュリティモジュール 3 2 からデコーダ 3 1 の復号器 4 2 に供給される。

【0038】デコーダ 3 1 側においては、復号器 4 2 が、入力された暗号化されているスクランブル鍵を復号化する。この復号化には、上述したように、セキュリティモジュール 3 2 の暗号器 5 4 において暗号化のために用いられた Card ID または Ca__System__ID が必要となるが、これらは図 5 を参照して後述するように、セキュリティモジュール 3 2 をデコーダ 3 1 に装着したとき、セキュリティモジュール 3 2 からデコーダ 3 1 に供給され、デコーダ 3 1 側において、記憶されている。

【0039】復号器 4 2 は、復号したスクランブル鍵を、デスクランブラ 4 1 に供給する。デスクランブラ 4 1 においては、スクランブルされている所定の番組のデジタル信号が、復号器 4 2 より供給されたスクランブル鍵（復号化されている）によってデスクランブルされ、正常に視聴可能な元の信号に戻された後、出力される。

【0040】図 4 の実施例における暗号器 5 4 と復号器 4 2 を省略した構成にすると、セキュリティモジュール 3 2 を他の装置で駆動し、その出力をメモリなどに取り込むようにすると、スクランブル鍵が第三者に不正に取得され、悪用されるおそれがある。しかしながら、実施例のように、暗号器 5 4 により暗号化した状態でスクランブル鍵を出力するようにしておくと、セキュリティモジュール 3 2 より出力されたスクランブル鍵を単に取り込んだだけでは、このスクランブル鍵は暗号化されているため、そのままでは用いることができない。従って、

スクランブル鍵の盗用を抑制することができる。

【0041】なお、デコーダ31は、これを分解すると、内部の回路が正常に動作しないように構成されたり、分解すると、分解されたことが視聴情報としてEEPROM53に記憶され、さらに視聴情報収集処理システム7に転送されるように構成されているので、デコーダ31の分解により、スクランブル鍵が盗用されるおそれは抑制されている。

【0042】次に、図5を参照して、ICカードで構成されるセキュリティモジュール32を、デコーダ31に装着した場合に行われる動作について説明する。

【0043】セキュリティモジュール32は、独自に動作を行うことがなく、常にデコーダ31からの指令に対応して、所定の返事を返す機能のみを有している。

【0044】デコーダ31は、セキュリティモジュール32が装着されたとき、最初に、Reset信号を発生し、セキュリティモジュール32に出力する。セキュリティモジュール32は、このReset信号が入力されると、リセット動作を行い、リセット動作が完了すると、Answer To Reset信号をデコーダ31に出力する。

【0045】デコーダ31は、このAnswer To Reset信号の入力を受け、セキュリティモジュール32のリセットが完了したことを検知すると、次に、セキュリティモジュール32に対して、ID Request信号を出力する。セキュリティモジュール32は、このID Request信号の入力を受けたとき、EEPROM53に記憶されているCard IDとCa_System_IDをデコーダ31に出力する。

【0046】このCard IDは、セキュリティモジュール32に個別に与えられたセキュリティモジュール32に固有のIDである。セキュリティモジュール32は、受信した個別情報のうち、自分自身の個別情報として、EEPROM53に取り込むべき個別情報であるのか否かを判定するのに、このCard IDを用いている。

【0047】一方、Ca(Conditional access)_System_IDは、複数の限定受信システムが共存する場合において、各受信システムを識別するための識別子である。

【0048】デコーダ31は、このCard IDとCa_System_IDが供給されたとき、これを内蔵するRAMに記憶する。そして、上述したように、これらを復号器42における復号の鍵として用いるようにする。

【0049】次に、デコーダ31は、受信した個別情報(EMM:Entitlement Management Message)をセキュリティモジュール32に出力する。セキュリティモジュール32は、この個別情

報(EMM)の入力を受けたとき、Card IDに対応するものを抽出し、対応するResponseをデコーダ31に返す。

【0050】また、デコーダ31は、番組情報(ECM:Entitlement Control Message)を、セキュリティモジュール32に出力する。セキュリティモジュール32は、供給された番組情報から、上述したように、スクランブル鍵Ksを復号し、これをさらに暗号化して、デコーダ31に出力する。

【0051】セキュリティモジュール32は、スクランブル鍵Ks以外にも、Copy RightとFinger Printingを、デコーダ31に出力する。このCopy Rightは、対応する番組をコピーすることが許可されているか否かを表すフラグである。また、Finger Printingは、その番組に対応されているCard IDを強制的にモニタに表示させるか否かを表すフラグである。

【0052】以下、デコーダ31より個別情報(EMM)が供給されると、セキュリティモジュール32は、それに対応するメッセージを返し、また、デコーダ31より番組情報(ECM)が供給されると、セキュリティモジュール32は、対応するメッセージを返す動作が適宜行われる。

【0053】上記実施例においては、伝送路23を放送波であるものとして説明したが、これに限定されるものではなく、光ファイバケーブルやその他の伝送媒体とすることも可能である。

【0054】また、暗号器54と復号器42で用いる鍵としては、Card IDまたはCa_System_ID以外のものを用いることも可能である。ただし、これらを用いれば、これらはセキュリティモジュール32からデコーダ31に最初に必ず伝送されるものなので、他の鍵を設定した場合のように、その鍵を伝送するシーケンスを新たに追加する必要がない。

【0055】

【発明の効果】請求項1に記載のデスクランブル装置および請求項2に記載のデスクランブル方法によれば、抽出手段において、スクランブル鍵を暗号化してデスクランブル手段に供給し、デスクランブル手段において、暗号化されたスクランブル鍵を、復号化するようにしたので、スクランブル鍵が不用意に解読され、悪用されるのを抑制することができる。

【図面の簡単な説明】

【図1】本発明を応用した有料放送システムの構成例を示すブロック図である。

【図2】個別情報の一部を示す図である。

【図3】番組情報の一部を示す図である。

【図4】図1の受信端末22の動作の原理を説明するための図である。

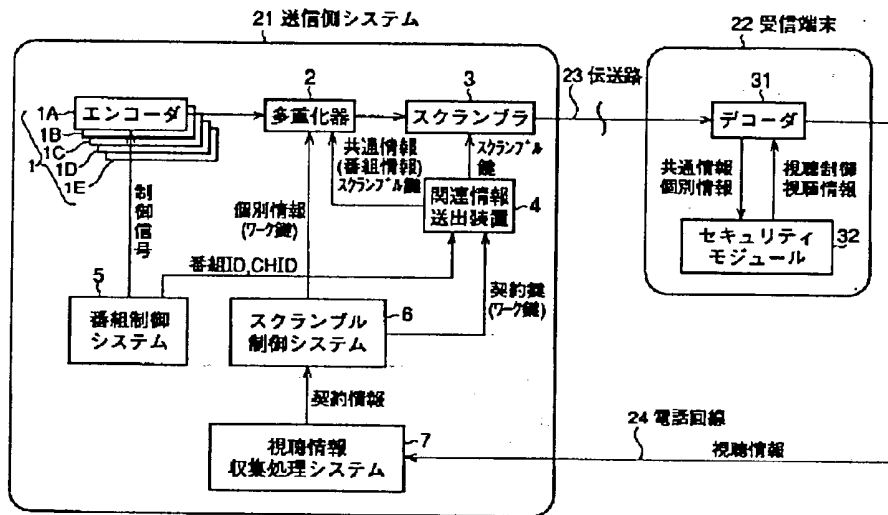
【図 5】図 1 のデコーダ 3 1 とセキュリティモジュール 3 2 の間の信号の授受を説明する図である。

【符号の説明】

1. 1 A 乃至 1 E エンコーダ
- 2 多重化器
- 3 スクランプラ
- 4 関連情報送出装置
- 5 番組制御システム
- 6 スクランプル制御システム
- 7 視聴情報収集処理システム

- 2 1 送信側システム
- 2 2 受信端末
- 2 3 伝送路
- 2 4 電話回線
- 3 1 デコーダ
- 3 2 セキュリティモジュール
- 4 1 デスクランブラ
- 4 2, 5 1, 5 2 復号器
- 5 3 EEPROM
- 10 5 4 暗号器

【図 1】



【図 2】

契約鍵番号	契約鍵	service_id	契約タイプ
8ビット	64ビット	16ビット	4ビット

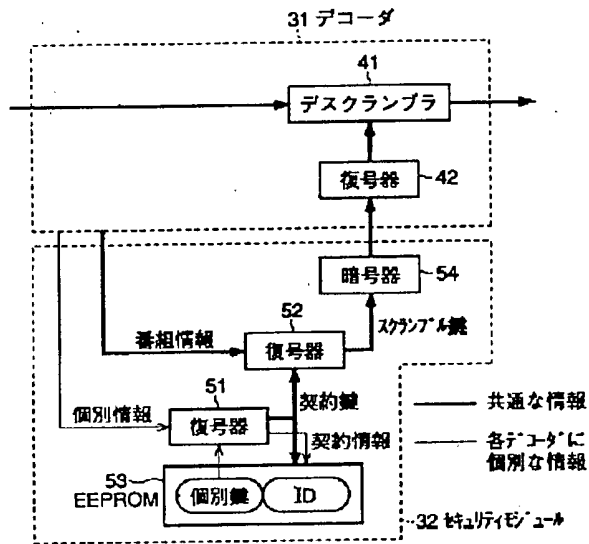
個別情報

【図 3】

契約タイプ	契約鍵番号	スクランブル鍵(暗号化)	service_id	番組ID
4ビット	8ビット	64ビット	16ビット	16ビット

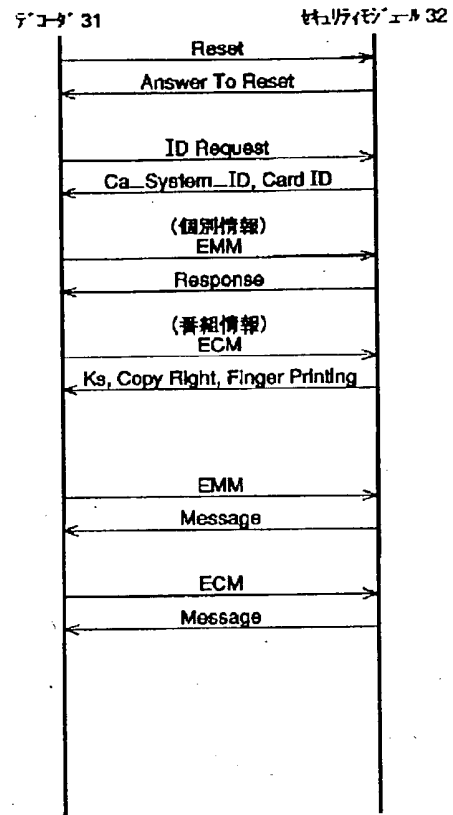
番組情報

【図 4】



受信端末 22

【図 5】



This Page Blank (uspto)

This Page Blank (uspto)